Chaotic Filter Bank for Computer Cryptography

Bingo Wing-Kuen Ling

Telephone: 44 (0)20 78482294 Fax: 44 (0)20 78482932 Email: wing-kuen.ling@kcl.ac.uk

Department of Electronic Engineering, Division of Engineering, King's College London, Strand, London, WC2R 2LS, United Kingdom.

Charlotte Yuk-Fan Ho

Telephone: 44 (0)20 78827986 Fax: 44 (0)20 78827997 Email: charlotte.ho@elec.qmul.ac.uk

Department of Electronic Engineering, Queen Mary, University of London, Mile End Road, London, E1 4NS, United Kingdom.

Peter Kwong-Shun Tam

Telephone: 852 27666238 Fax: 852 23628439 Email: enptam@polyu.edu.hk

Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong, PRC.

Abstract

A chaotic filter bank for computer cryptography is proposed. By encrypting and decrypting signals via a chaotic filter bank, the following advantages are enjoyed: 1) one can embed signals in different frequency bands by employing different chaotic functions; 2) the number of chaotic generators to be employed and their corresponding functions can be selected and designed in a flexible manner because perfect reconstruction does not depend on the invertibility, causality, linearity and time invariance of the corresponding chaotic functions; 3) the ratios of the subband signal powers to the chaotic subband signal powers can be easily changed by the designers and perfect reconstruction is still guaranteed no matter how small these ratios are; 4) the proposed cryptographical system can be easily adapted in the international multimedia standards, such as JPEG 2000 and MPEG4.

1. Introduction

Cryptography using chaos found many applications in audio processing [Delgado-Restituto, 1996], image processing [Yen, 2000] and communications [Yang, 1997]. The existing cryptographical algorithms are implemented based on chaotic oscillator [Delgado-Restituto, 1996], Chua's circuit [Yang, 1997], modulo operator [Götz, 1997; Dachselt, 1998] and permutation scheme [Yen, 2000]. However, these

algorithms are formulated based on the time domain state space nonlinear differential or difference equations. Hence, the information of the signals at different frequency bands does not exploited. Moreover, although these existing nonlinear cryptographical systems produce uncorrelated signals, these methods are highly relied on the corresponding chaotic functions. Hence, details analysis of these chaotic functions, such as the stability regions of chaotic parameters, sensitivity of these parameters to rounding errors, invertibility of the chaotic functions etc, is required. Unfortunately, the stability regions of parameters of the existing chaotic functions are limited and these parameters are very sensitive to rounding errors. Hence, it would cause significant errors and disasters when these methods are applied to real systems. Furthermore, since the structures of the existing chaotic systems are not flexible in the sense of changing the number of chaotic generators and their corresponding functions. Hence, the order of the complexity of the encrypted signals is constrained. In addition, these systems cannot be adapted into the existing international multimedia standards directly because the existing international multimedia standards are based on the filter bank approach.

On the other hand, filter bank and wavelets theory is widely studied and found many applications in many engineering disciplines, particularly in multimedia signal processing applications [Vaidyanathan, 1990; Phoong, 1995; Mao, 2000; Soman, 1993]. This is because filter bank and wavelets theory exploits both the time domain and frequency domain information of the signals. By permuting the subband signals, the signals are encrypted. Although both the encryption and decryption of this method is simple because just matrix multiplications are involved, the encrypted signal is usually correlated to the input signal. This is because since the power spectrum density of the input signal is usually not flat, permuting the subband signals cannot flatten the power spectral density. Recently, the filter bank and wavelets theory are extended to the systems with nonlinearity [Redmill, 1996]. Redmill found that perfect reconstruction can be achieved no matter the corresponding subband processing are noninvertible, noncausal, nonlinear and time varying. Also, the filter system is very flexible in the sense of changing the number of subband processing units and their corresponding functions. However, Redmill does not explore any applications.

In this paper, a chaotic filter bank for computer cryptography is proposed. Our proposed system enjoys both the advantages of the traditional filter bank approach

and the existing nonlinear chaotic approach because the chaotic functions can produce an uncorrelated signal and the filter bank structure ensures perfect reconstruction no matter the chaotic functions are noninvertible, noncausal, nonlinear and time varying. The outline of this paper is as follows: The cryptographical system is discussed in section 2 and simulation results are given in section 3. Finally, a conclusion is summarized in section 4.

2. Proposed cryptographical system

Refer to figure 1: let $x[n]$ and $y[n]$ be the input and the reconstructed signal of the filter bank system; $t_0[n]$ and $t_1[n]$ be the subband signals decomposed by the analysis bank; $v_0[n]$ and $v_1[n]$ be the encrypted subband signals; $w_0[n]$ and $w_1[n]$ be the decrypted subband signals; $H_i(z)$ and $F_i(z)$ for $i = 0,1$ be the analysis filters and synthesis filters; $\downarrow 2$ and $\uparrow 2$ be a 2-fold decimator and 2-fold expander; K_0 and K_1 be the gains multiplied on each channels; and $\alpha_i(\cdot)$ for $i = 0,1$ be the chaotic functions, respectively.

The various signals in figure 1 can be expressed as follows:

$$t_0[n] = K_0 \sum_{\forall m} x[m] h_0[2n - m], \tag{1}$$

$$t_1[n] = K_1 \sum_{\forall m} x[m] h_1[2n - m], \tag{2}$$

$$v_0[n] = t_0[n] + \alpha_0(t_1[n]), \tag{3}$$

$$v_1[n] = t_1[n] - \alpha_1(v_0[n]), \tag{4}$$

$$w_1[n] = v_1[n] + \alpha_1(v_0[n]) = t_1[n], \tag{5}$$

$$w_0[n] = v_0[n] - \alpha_0(w_1[n]) = t_0[n], \tag{6}$$

and

$$y[n] = \frac{1}{K_0} \sum_{\forall m} w_0[m] f_0[n - 2m] + \frac{1}{K_1} \sum_{\forall m} w_1[m] f_1[n - 2m]. \tag{7}$$

A filter bank is said to achieve perfect reconstruction if $y[n]$ is a delayed gain version of $x[n]$. That is, $\exists c \in \Re$ and $\exists m_0 \in Z$ such that $y[n] = cx[n - m_0]$ $\forall n \in Z$. This property is important in cryptography because this guarantees decryption is lossless. It is shown in [Redmill, 1996] that the filter bank system achieves perfect reconstruction if and only if

$$\frac{1}{2}\begin{bmatrix} H_0(z) & H_1(z) \\ H_0(-z) & H_1(-z) \end{bmatrix}\begin{bmatrix} F_0(z) \\ F_1(z) \end{bmatrix} = \begin{bmatrix} cz^{-m_0} \\ 0 \end{bmatrix}, \tag{8}$$

no matter $\alpha_i(\cdot)$ for $i = 0,1$ are noninvertible, noncausal, nonlinear and time varying functions. This property provides a great flexibility in design because one can embed signals in different frequency bands by employing different chaotic functions, and the number of chaotic generators as well as their corresponding functions can be selected and designed in a more flexible manner.

By expressing the filters in the polyphase representation, that is

$$H_i(z) = \sum_{l=0}^{1} z^{-l} E_{i,l}(z^2) \tag{9}$$

and

$$F_i(z) = \sum_{l=0}^{1} z^{l-1} R_{l,i}(z^2), \tag{10}$$

for $i = 0,1$, the perfect reconstruction condition becomes

$$\mathbf{R}(z)\mathbf{E}(z) = cz^{-m_0}\mathbf{I}, \tag{11}$$

where $\mathbf{I}$ is an identity matrix [Vaidyanathan, 1990].

It is found that if $\mathbf{E}(z)$ is a paraunitary matrix, that is

$$\tilde{\mathbf{E}}(z)\mathbf{E}(z) = d\mathbf{I}, \tag{12}$$

where d is a constant and $\tilde{\mathbf{E}}(z)$ denotes $\mathbf{E}_*^T(z^{-1})$ in which $\mathbf{E}_*(z)$ represents the conjugation of the coefficients of $\mathbf{E}(z)$, then the wavelets generated by the binary tree structure filter bank is orthonormal [Soman, 1993]. Since Haar wavelets is the unique wavelets function that is orthogonal, symmetrical, and of compact support. This wavelets function is chosen in our case. The mother wavelets function of Haar transform and the corresponding polyphase matrix are

$$\psi(t) = \begin{cases} 1 & 0 < t < 0.5 \\ -1 & 0.5 < t < 1 \\ 0 & otherwise \end{cases}, \tag{13}$$

and

$$\mathbf{E}(z) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{14}$$

respectively.

In order to generate uncorrelated signals, we employ the logistic maps as the

chaotic functions. The nonlinear functions are

$$x_i(k+1) = \lambda_i x_i(k)(1 - x_i(k)), \tag{15}$$

$$y_i(k) = x_i(k) + u_i(k), \tag{16}$$

for $i = 0,1$, where λ_i, $x_i(k)$, $u_i(k)$ and $y_i(k)$ are the parameters, state variables, inputs and outputs of the function $\alpha_i(\cdot)$, respectively. It is worth noting that $\alpha_i(\cdot)$ is in general not invertible, and chaotic behaviors are exhibited if $0 < x_i(0) < 1$ and $3 < \lambda_i < 4$. Hence, the parameters and the initial conditions are selected in these ranges for our case. In the cryptographical system, λ_i is used as the public keys, and $x_i(0)$ is used as private keys. Since the logistic map is very sensitive to both λ_i and $x_i(0)$ because of its chaotic nature, different users will get very different encrypted signals and they cannot decrypt other users' signals by using its own private keys.

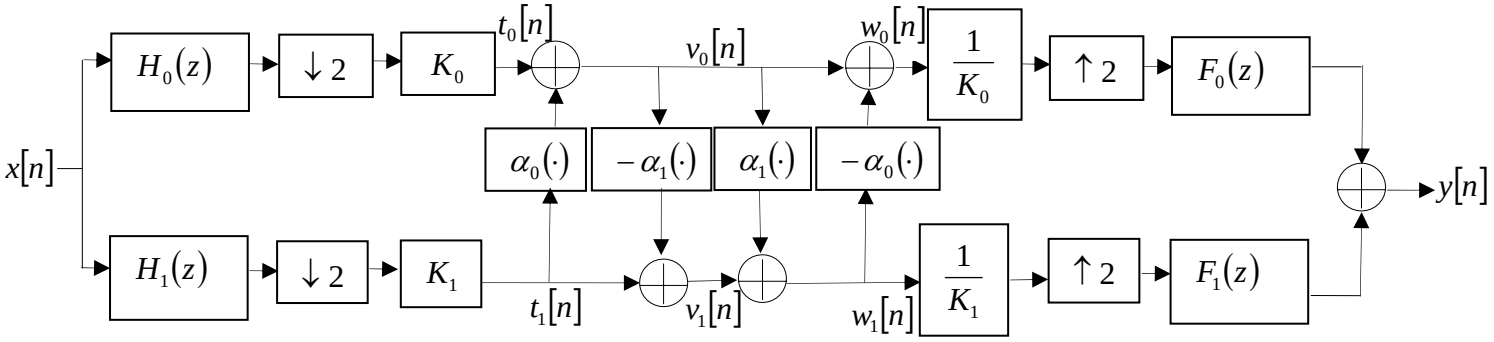

Figure 1. The proposed chaotic filter bank system.

3. Simulation results

In this paper, we choose a standard one dimensional test signal [Mallat, 1992], a simple sinusoidal signal and a random Gaussian noise with zero mean and unit variance as test inputs. The parameters are selected as $K_0 = 0.01$, $K_1 = 0.04$, $\lambda_0 = 3.98$, $\lambda_1 = 4$, $x_0(0) = 0.7$, $x_1(0) = 0.9$, $c = 1$ and $m_0 = 0$, respectively. The simulation results are shown in figures 2, 3 and 4, respectively. The correlation coefficients ($\frac{\sigma_{t_i v_j}}{\sqrt{\sigma_{t_i}^2 \sigma_{v_j}^2}}$) are summarized in table 1. According to the results shown in table 1, the encrypted subband signals are almost uncorrelated to the subband signals decomposed by the analysis bank, which implies that the encryption performance is very good.

Table 2 summarizes the ratios of subband signal power ($\sum_{\forall n}|t_i[n]^2$) to the subband chaotic signal power ($\sum_{\forall n}|v_i[n]-t_i[n]^2$) for each channel in the filter bank system. It is interesting to note that although these ratios are very low, perfect reconstruction is still guaranteed. Also, the designers can easily change these ratios by changing the values of K_0 and K_1, respectively.

	One dimensional test signal [Mallat, 1992]	Simple sinusoidal signal	Random Gaussian noise
$\frac{\sigma_{t_0 v_0}}{\sqrt{\sigma_{t_0}^2 \sigma_{v_0}^2}}$	-0.0002	0.0572	0.1177
$\frac{\sigma_{t_0 v_1}}{\sqrt{\sigma_{t_0}^2 \sigma_{v_1}^2}}$	0.0352	-0.0073	0.0038
$\frac{\sigma_{t_1 v_0}}{\sqrt{\sigma_{t_1}^2 \sigma_{v_0}^2}}$	0.2011	-0.0001	0.2582
$\frac{\sigma_{t_1 v_1}}{\sqrt{\sigma_{t_1}^2 \sigma_{v_1}^2}}$	-0.0908	-0.0014	0.0292

Table 1. Correlation coefficients of subband signals decomposed by analysis bank and encrypted subband signals.

	One dimensional test signal [Mallat, 1992]	Simple sinusoidal signal	Random Gaussian noise
$\frac{\sum_{\forall n}\|t_0[n]^2}{\sum_{\forall n}\|v_0[n]-t_0[n]^2}$	0.0011	0.00047599	0.00042144
$\frac{\sum_{\forall n}\|t_1[n]^2}{\sum_{\forall n}\|v_1[n]-t_1[n]^2}$	0.000019036	0.0000014244	0.0019

Table 2. Ratios of subband signal power to the subband chaotic signal power.

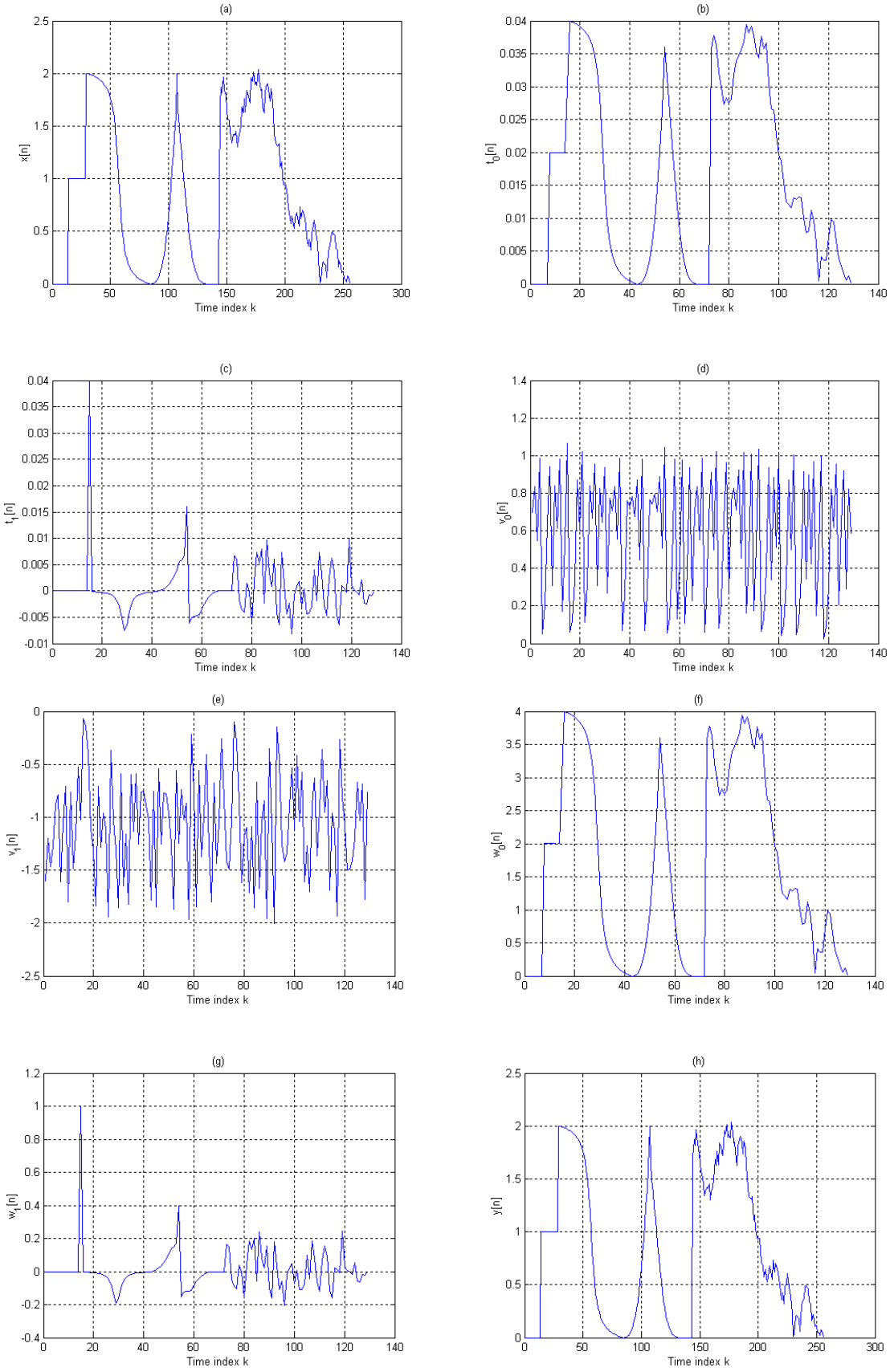

Figure 2. A one dimensional test signal [Mallat, 1992]. (a) $x[n]$. (b) $t_0[n]$. (c) $t_1[n]$. (d) $v_0[n]$. (e) $v_1[n]$. (f) $w_0[n]$. (g) $w_1[n]$. (h) $y[n]$.

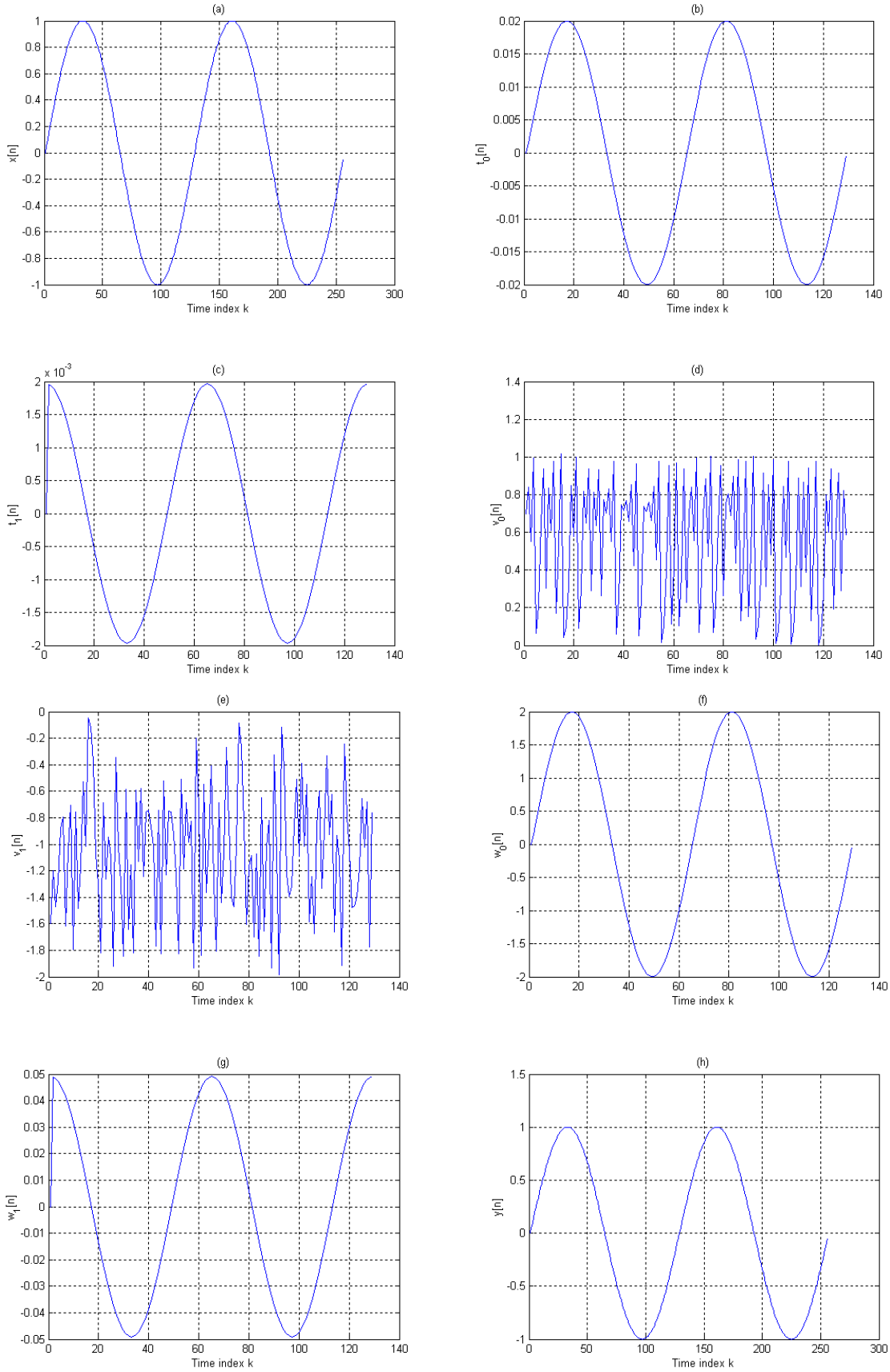

Figure 3. A simple sinusoidal signal. (a) $x[n]$. (b) $t_0[n]$. (c) $t_1[n]$. (d) $v_0[n]$. (e) $v_1[n]$. (f) $w_0[n]$. (g) $w_1[n]$. (h) $y[n]$.

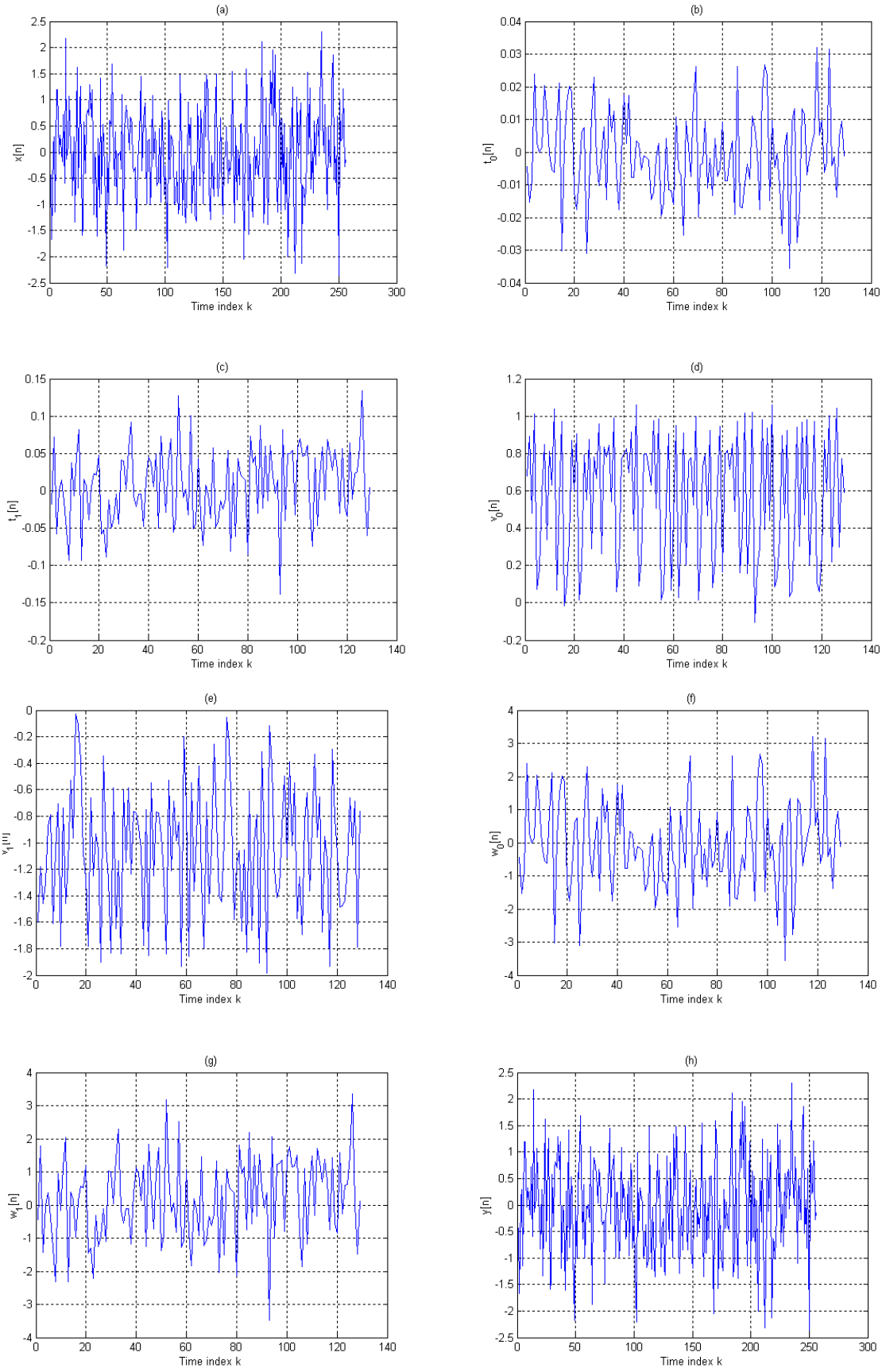

Figure 4. A random Gaussian noise with zero mean and unit variance. (a) $x[n]$. (b) $t_0[n]$. (c) $t_1[n]$. (d) $v_0[n]$. (e) $v_1[n]$. (f) $w_0[n]$. (g) $w_1[n]$. (h) $y[n]$.

4. Conclusion

In this paper, a chaotic filter bank system is proposed for computer cryptography. According to the simulation results, the system provides good performances for cryptography. Moreover, the system also provides high design flexibility.

Acknowledgement

The work described in this paper was substantially supported by The Hong Kong Polytechnic University.

References

[1] Dachselt, F., Kelber, K. and Schwarz, W. [1998], "Discrete-Time Chaotic Encryption Systems—Part III: Cryptographical Analysis," *IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications*, vol. 45, no. 9, pp. 983-988.

[2] Delgado-Restituto, M., Liñán, M. and Rodríguez-Vázquez, A. [1996], "CMOS 2.4μm Chaotic Oscillator: Experimental Verification of Chaotic Encryption of Audio," *Electronic Letters*, vol. 32, no. 9, pp. 795-796.

[3] Götz, M., Kelber, K. and Schwarz, W. [1997], "Discrete-Time Chaotic Encryption Systems—Part I: Statistical Design Approach," *IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications*, vol. 44, no. 10, pp. 963-970.

[4] Mallat, S. and Hwang, W. L. [1992], "Singularity Detection and Processing with Wavelets," *IEEE Transactions on Information Theory*, vol. 38, no. 2, pp. 617-643.

[5] Mao, J. S., Chan, S. C., Liu, W. and Ho, K. L. [2000], "Design and Multiplier-Less Implementation of a Class of Two-Channel PR FIR Filterbanks and Wavelets with Low System Delay," *IEEE Transactions on Signal Processing*, vol. 48, no. 12, pp. 3379-3394.

[6] Phoong, S. M., Kim. C. W., Vaidyanathan, P. P. and Ansari, R. [1995], "A New Class of Two-Channel Biorthogonal Filter Banks and Wavelet Bases," *IEEE Transactions on Signal Processing*, vol. 43, no. 3, pp. 649-665.

[7] Redmill, D. W. and Bull, D. R. [1996], "Nonlinear Perfect Reconstruction Critically Decimated Filter Banks," *Electronic Letters*, vol. 32, no. 4, pp. 310-311.

[8] Soman, A. K. and Vaidyanathan, P. P. [1993], "On Orthonormal Wavelets and Paraunitary Filter Banks," *IEEE Transactions on Signal Processing*, vol. 41, no. 3, pp. 1170-1183.

[9] Vaidyanathan, P. P. [1990], "Multirate Digital Filters, Filter Banks, Polyphase Networks, and Applications: A Tutorial," *IEEE Proceedings*, vol. 78, no. 1, pp. 56-93.

[10] Yang, T., Wu, C. W. and Chua, L. O. [1997], "Cryptography Based on Chaotic Systems," *IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications*, vol. 44, no. 5, pp. 469-472.

[11] Yen, J. C. and Guo, J. I. [2000], "Efficient Hierarchical Chaotic Image Encryption Algorithm and its VLSI Realisation," *IEE Proceedings—Vision, Image and Signal Processing*, vol. 147, no. 2, pp. 167-175.